

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

**Template Version 1.0, Released on 2017-06-21**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 23/05/2018 | 1.0 | Trijeet | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Technical Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Technical Safety Concept](#_757cx6xm46zb)

[Functional Safety Requirements](#_2f9rjqxbsp2)

[Refined System Architecture from Functional Safety Concept](#_qp3s9pvua9mt)

[Functional overview of architecture elements](#_cqb49updinx4)

[Technical Safety Concept](#_mx8us8onanqo)

[Technical Safety Requirements](#_lnxjuovv6kca)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Technical Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Technical Safety Concept

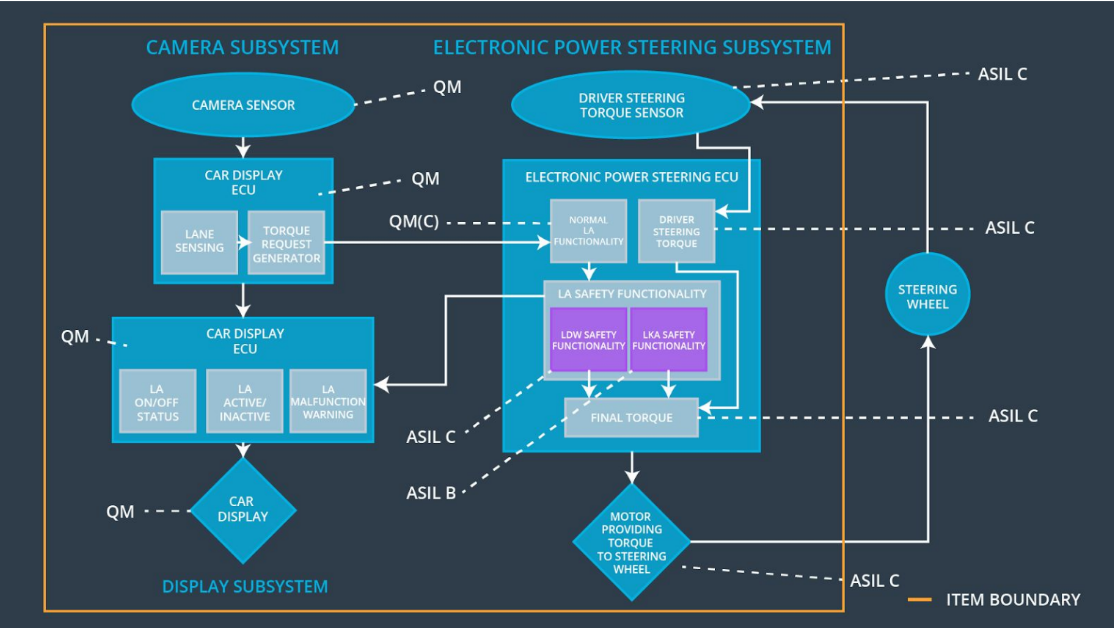
The purpose of the functional safety concept is to identify the high level system requirements without diving deep into the technical aspects. Different parts of the item architecture are allocated with the responsibility of fulfilling these requirements. The result of this leads to construction of the technical safety requirements from it. Validation and verification instructions for these requirements are also laid down in this. Finally, these requirements will be considered while hardware and software implementation of the system.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The lane keeping assistance function shall ensure that the lane departure oscillating torque amplitude stays below Max\_Torque\_Amplitude | C | 50 ms | Oscillation torque amplitude maintained below Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The lane keeping assistance function shall ensure that the lane departure oscillating torque frequency stays below Max\_Torque\_Frequency | C | 50 ms | Oscillation torque amplitude maintained below Max\_Torque\_Frequency |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for no more than Max\_Duration so that the driver cannot misuse the system for autonomous driving | B | 500 ms | Disable the lane keeping assistance function |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures the scene in front of the car and feeds the image to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Detects the lane lines in the image from the Camera Sensor feed. |
| Camera Sensor ECU - Torque request generator | Calculates the amount of torque required and requests the same to the Electronic Power Steering ECU. |
| Car Display | Displays warning notifications as fed from Car Display ECU |
| Car Display ECU - Lane Assistance On/Off Status | Indicates whether the Lane Assistance is turned on or off. |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates whether the Lane Assistance is currently being used (active) or not (inactive). |
| Car Display ECU - Lane Assistance malfunction warning | Indicates whether the Lane Assistance has malfunctioned. |
| Driver Steering Torque Sensor | Detects the amount of torque being applied by the driver on the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Receives the torque applied by the driver as detected by the Driver Steering Torque Sensor. |
| EPS ECU - Normal Lane Assistance Functionality | Receives the torque request from the Camera Sensor ECU - Torque request generator and provides Lane Keeping Assistance and Lane Departure Warnings |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensures that the torque amplitude and frequency are below Max\_Torque\_Amplitude and Max\_Torque\_Frequency respectively. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensures that the torque request is not active for more than Max\_Duration. |
| EPS ECU - Final Torque | Computes the effective torque required by combining the torque request from the Lane Departure Warning and Lane Keeping Assistance functions. |
| Motor | Applies the necessary torque as computed by EPS ECU - Final Torque onto the steering wheel. |

# Technical Safety Concept

## Technical Safety Requirements

**Lane Departure Warning (LDW) Requirements:**

Functional Safety Requirement 01-01 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component shall ensure that the amplitude of the ‘LDW\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Amplitude’ | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | As soon as failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW\_Torque\_Request’ shall be set to zero. | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | As soon as the LDW function deactivates the LDW feature, the ‘LDW Safety’ software block shall send a signal to the car display ECU to turn on a warning light | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity for the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50 ms | Data Transmission Integrity Check | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory | A | Ignition cycle | Safety Startup | LDW\_Torque\_Request is set to zero. |

Functional Safety Requirement 01-2 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component shall ensure that the frequency of the ‘LDW\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Frequency | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | As soon as failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW\_Torque\_Request’ shall be set to zero. | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | As soon as the LDW function deactivates the LDW feature, the ‘LDW Safety’ software block shall send a signal to the car display ECU to turn on a warning light | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity for the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50 ms | Data Transmission Integrity Check | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory | A | Ignition cycle | Safety Startup | LDW\_Torque\_Request is set to zero. |

**Lane Keeping Assistance (LKA) Requirements:**

Functional Safety Requirement 02-1 with its associated system elements

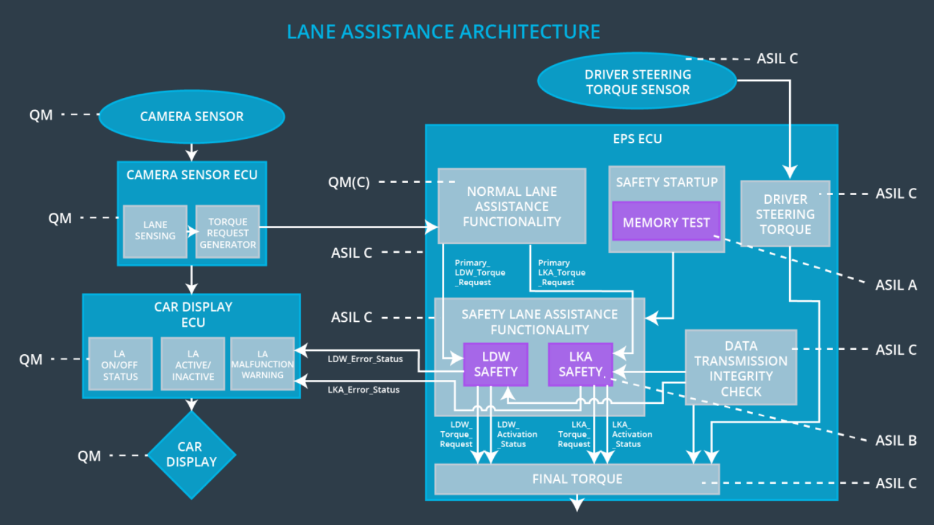
(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | The LKA safety component shall ensure that the duration of the ‘LKA\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Duration’ | B | 500 ms | LKA Safety | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | As soon as failure is detected by the LKA function, it shall deactivate the LKA feature and the ‘LKA\_Torque\_Request’ shall be set to zero. | B | 500 ms | LKA Safety | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | As soon as the LKA function deactivates the LKA feature, the ‘LKA Safety’ software block shall send a signal to the car display ECU to turn on a warning light | B | 500 ms | LKA Safety | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity for the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured | B | 500 ms | Data Transmission Integrity Check | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory | A | Ignition cycle | Safety Startup | LKA\_Torque\_Request is set to zero. |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disable lane departure warning | Malfunction\_01,  Malfunction\_02 | Yes | Alert on car display: Lane Departure Warning Malfunction |
| WDC-02 | Disable lane keeping assistance | Malfunction\_03 | Yes | Alert on car display: Lane Keeping Assistance Malfunction |